RAPPEL ETHERNET

Format des adresses :

L'adresse MAC contient 6 octets.

- Le premier octet transmis est l'octet zéro.
- Le premier bit transmis est nommé I/G. Valeur à zéro il indique une adresse Individuelle, valeur à 1 indique une adresse de groupe.
- Le 2eme bit transmis est nommé U/L. Valeur à zéro il indique une adresse Universelle (unique dans le monde), valeur à 1 une adresse Locale.

```
Ethernet II, Src: SamsungE_ab:96:28 (80:18:a7:ab:96:28), Dst: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
  Destination: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
      Address: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
      Address: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

Les 3 premiers octets 0 à 2, nommés OUI pour Organizationally Unique Identifier identifient de manière unique une organisation. Leur valeur est assignée par une autorité d'enregistrement.

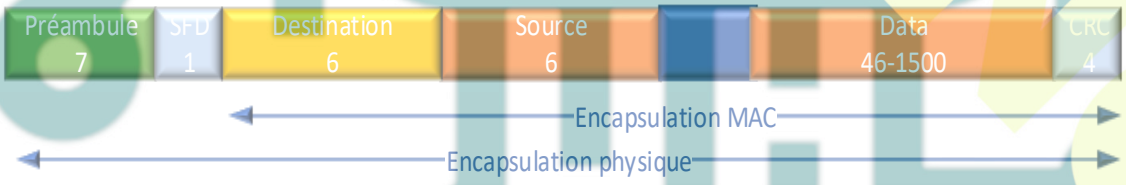
Les octets 3 4 5 sont assignés par l'organisation pour numéroter ses cartes.

Le format de la trame ETHERNET

- **Informations de la couche physique**

7 octets de préambule qui vont être utilisés par le récepteur pour se synchroniser dans la version 10 Mb/s des 1 et des 0, pour la version à 100 Mbps seront remplacés par des symboles J, K.

Une fois le préambule transmis, l'émetteur va transmettre la séquence **starting frame delimiter** (1 octet) que le récepteur va être capable de décoder. A ce moment il est prêt à décoder les informations qui vont suivre dans la trame.



Les informations suivantes sont les 12 octets d'adresse : 6 octets d'adresse destination suivis de 6 octets d'adresse source et 4 octets de CRC à la fin de la trame pour vérifier qu'il n'y a pas eu d'erreur de transmission. Cette trame MAC contient également deux champs : un champ dit longueur/type et un champ de Padding. Le champ Padding (bourrage) permet d'atteindre la valeur minimale de la trame (64 octets) si le message est trop petit.

Le champ longueur/type qui, a un double rôle en fonction de l'architecture Ethernet qui va être utilisée. Le récepteur va donc devoir comprendre les données, et pour cela il va utiliser ce champ.

- **Architecture Ethernet DIX (constructeur)**

Elle va transmettre les données sans utiliser de couches LLC et donc utiliser le champ type. On reconnait le champ type parce que sa valeur est supérieure à 1536. Comme les longueurs de trame Ethernet sont inférieures à 1518 le protocole sait que ce qui suit n'est pas une encapsulation de type LLC.


```
Ethernet II, Src: SamsungE_ab:96:28 (80:18:a7:ab:96:28), Dst: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
  Destination: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
      Address: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
      Address: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

- **Architecture Ethernet 802.3 (IEEE)**

Envoie les informations dans une sous couche LLC et va utiliser le champ longueur. Nous voyons le champ L/T et derrière nous aurons les 3 octets de l'encapsulation LLC.

DSAP (Destination Service Access Point), désigne le protocole supérieur destinataire des données.

SSAP (Source Service Access Point), désigne le protocole qui a émis la trame LLC. Vous avez les valeurs AA pour le DSAP, AA pour le SSAP, et 03 pour CTRL.

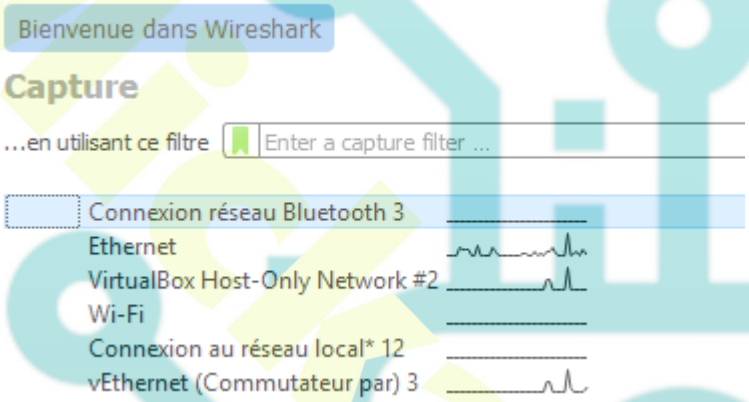
```
IEEE 802.3 Ethernet
  Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
  Source: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
  Length: 38
  Padding: 0000000000000000
Logical-Link Control
  DSAP: Spanning Tree BPDU (0x42)
  SSAP: Spanning Tree BPDU (0x42)
  Control field: U, func=UI (0x03)
```

Analyse de trames Ethernet

Installer WIRESHARK (machine perso ou Windows virtualisé)

https://www.wireshark.org/download.html

1. Dans l'écran de bienvenue, choisir l'interface réseau à utiliser (ETHERNET ou connexion réseau local)

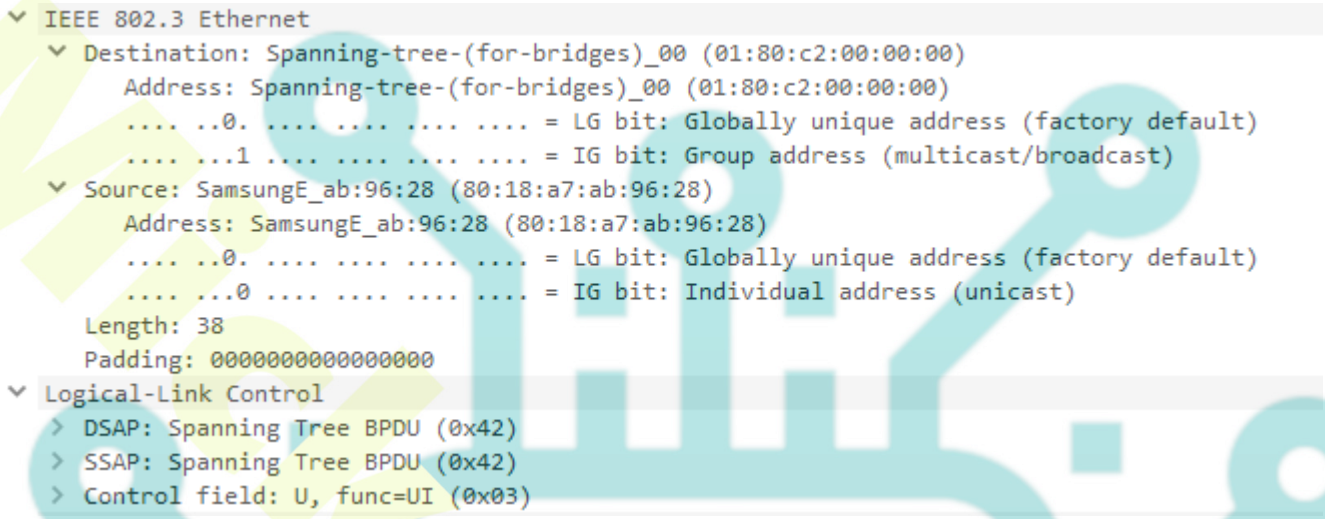


2. Dans le menu CAPTURE, choisir DEMARRER
3. Laisser tourner la capture 20 secondes environ
4. Puis, dans le menu CAPTURE, choisir ARRETER

Exercice 1 - On cherche maintenant une trame de type 802.3

Dans le menu EDITER, sélectionner TROUVER UN PAQUET et saisissez LLC

Développer IEE 802.3 et Logical Link Control (comme sur le schéma suivant)

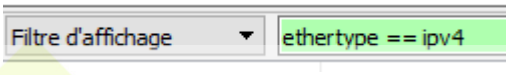


Questions ETHERNET 802.3

1. Quelle est l'adresse source et l'adresse de destination ?
2. L'adresse de destination est une adresse individuelle ou une adresse de groupe (BIT I/G) ?
3. L'adresse source est une adresse universelle ou une adresse locale (BIT U/L nommé LG dans WireShark) ?
4. Le protocole 802.3 possède-t-il un champ LLC ?
5. Ce champ contient-il les données DSAP, SSAP, CTRL ?
6. Les valeur DSAP et SSAP valent-elles AA ? (Prendre la calculette programmeur pour convertir)
7. Le champ CTRL est-il égale à 3 ?
8. Quel protocole de couche supérieure est indiqué dans les champs DSAP et SSAP ?

Exercice 2 -On cherche maintenant une trame de type Ethernet II (DIX)

Dans le filtre d'affichage, saisir la valeur…



Déployer Ethernet II

```
Ethernet II, Src: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36), Dst: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
  Destination: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
      Address: SamsungE_ab:96:28 (80:18:a7:ab:96:28)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
      Address: Micro-St_f0:c4:36 (44:8a:5b:f0:c4:36)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
```

Questions EHERNET II

1. Quelle est l'adresse source et l'adresse de destination ?
2. L'adresse de destination est une adresse individuelle ou une adresse de groupe (BIT I/G) ?
3. L'adresse source est une adresse universelle ou une adresse locale (BIT U/L nommé LG dans WireShark) ?
4. Le protocole Ethernet II possède-t-il un champ LLC ?
5. Le protocole Ethernet II possède-t-il un champ TYPE ?
6. Quelle est la valeur du champ TYPE ?
7. A votre avis que contient le champ données ?

ATELIER ARP

Hardware type
Ce champ est placé en premier afin d'indiquer quel est le format de l'entête Arp.

- 01 – Ethernet (10Mb)
- 06 – IEEE 802 Networks
- 16 – Asynchronous Transmission Mode (ATM)
- 31 – IPsec tunnel [RFC3456]

Protocol type
Ce champ indique quel est le type de protocole couche 3 qui utilise Arp. Voici la valeur propre à IP (0x0800 – IP)

Hardware Address Length
Ce champ correspond à la longueur de l'adresse physique. La longueur doit être prise en octets. (06 – Ethernet)

Protocol Address Length
Ce champ correspond à la longueur de l'adresse réseau. La longueur doit être prise en octets. (04 – IP v4 et 16 – IP v6)

Operation
Ce champ permet de connaître la fonction du message et donc son objectif. Voici les différentes valeurs possibles. (01 – Request et 02 – Reply)

Sender Hardware Address
Ce champ indique l'adresse physique de l'émetteur. Dans le cadre spécifique d'Ethernet, cela représente l'adresse Mac source.

Sender Internet Address
Ce champ indique l'adresse réseau de l'émetteur. Dans le cadre spécifique de TCP/IP, cela représente l'adresse Ip de source.

Target Hardware Address
Ce champ indique l'adresse physique du destinataire. Dans le cadre spécifique d'Ethernet, cela représente l'adresse Mac destination. Si c'est une demande Arp, alors, ne connaissant justement pas cette adresse, le champ sera mis à 0.

Target Internet Address
Ce champ indique l'adresse réseau du destinataire. Dans le cadre spécifique de TCP/IP, cela représente l'adresse IP de destination.

Questions ARP

Rechercher un message ARP request en lançant Wireshark puis taper la commande ping vers 8.8.8.8.

1. Quelle est l'adresse source IP et MAC
2. Quelle est l'adresse de destination MAC et IP ?
3. L'adresse de destination est-elle connue ?
4. Pourquoi ?
5. Quelle est la valeur du champ protocole ?
6. Quelle est la taille de l'adresse MAC et pourquoi ?
7. Quelle est la taille du protocole et pourquoi ?

Rechercher un message ARP reply correspondant à votre request

1. Quelle est l'adresse source IP et MAC
2. Quelle est l'adresse de destination MAC et IP ?
3. L'adresse MAC renvoyée correspond elle à l'adresse IP demandée ?

Rechercher un message ARP reply correspondant à votre request

Analyse ICMP

Type et Code

Les champs Type et Code représentent la définition de message d'erreur contenu. Voici la liste des principales combinaisons entre les champs Type et Code :

- type=00 et code=00 : Réponse à une demande d'écho
- type=03 et code=00 : Réseau inaccessible
- type=03 et code=01 : Hôte inaccessible
- type=03 et code=02 : Protocole inaccessible
- type=03 et code=03 : Port inaccessible
- type=03 et code=04 : Fragmentation nécessaire mais interdite
- type=03 et code=05 : Echec de routage par la source
- type=03 et code=06 : Réseau de destination inconnu
- type=03 et code=07 : Hôte de destination inconnue
- type=04 et code=00 : Volume de donnée trop importante
- type=05 et code=00 : Redirection pour un hôte
- type=05 et code=01 : Redirection pour un hôte et pour un service donné
- type=05 et code=02 : Redirection pour un réseau
- type=05 et code=03 : Redirection pour un réseau et pour un service donné
- type=08 et code=00 : Demande d'écho
- type=09 et code=00 : Avertissement routeur
- type=10 et code=00 : Sollicitation routeur
- type=11 et code=00 : Durée de vie écoulée avant d'arrivée à destination
- type=11 et code=01 : Temps limite de réassemblage du fragment dépassé
- type=12 et code=00 : Entête IP invalide
- type=12 et code=01 : Manque d'une option obligatoire
- type=12 et code=02 : Mauvaise longueur
- type=13 et code=00 : Requête pour un marqueur temporel
- type=14 et code=00 : Réponse pour un marqueur temporel
- type=15 et code=00 : Demande d'adresse réseau
- type=16 et code=00 : Réponse d'adresse réseau
- type=17 et code=00 : Demande de masque de sous réseau
- type=18 et code=00 : Réponse de masque de sous réseau

Question ICMP

Lancer la capture et taper la commande ping 8.8.8.8 puis ping 1.2.3.4 et tracert 8.8.8.8

1. Chercher le ping echo request correspondant au 8.8.8.8
2. Quelle est la valeur type et à quoi correspond-elle ?
3. Quelle est la valeur des datas ?

Chercher la capture correspondant au ping 1.2.3.4

1. Quelle est la valeur de security level ?

Chercher une capture correspondant au tracert

1. Quelle est la valeur du champ type ?

Analyse IP

Le champ Vers

Le champ version représente le numéro de version du protocole IP.

- 04 – IP V4, 06 – IP V6

IHL

IHL signifie « Internet header lengh » représente la longueur l'entête IP.

Service

Le champs service « Type Of Service » permet la gestion d'une qualité de service traitée directement en couche 3 d'OSI. Cependant, la plupart des équipements de Backbone, ne tiennent pas compte de ce champ et même certain le réinitialise à 0.

Priorité

Le champ Priorité « Precedence » indique la priorité que possède le paquet.

- 000 – Routine, 100 – Très urgent, 101 – Critique, 111 – Supervision réseau

Longueur totale

Le champ Longueur totale représente la longueur du paquet incluant l'entête IP et les Data associées.

Identification

Le champ Identification constitue l'identification utilisée pour reconstituer les différents fragments.

Flags

Le champ Flags indique l'état de la fragmentation. Voici le détail des différents bits constituant ce champ.

- Reserved
  Le premier bit est réservé et positionné à 0.
- DF
  Appelé DF « Don't Fragment », le second bit permet d'indiquer si la fragmentation est autorisée. Si un Datagramme devant être fragmenté possède le flag DF à 1, alors, il sera alors détruit.
- MF
  Appelé MF « More Fragments », le troisième bit indique s'il est à 1 que le fragment n'est pas le dernier.

Position fragment

Le champ Position fragment est codé sur 13 bits et indique la position du fragment par rapport à la première trame. Le premier fragment possède donc le champ Position fragment à 0.

TTL

Le champ TTL (Time To Live) est codé sur 8 bits et indique la durée de vie maximale du paquet. Il représente la durée de vie en seconde du paquet. Si le TTL arrive à 0, alors l'équipement qui possède le paquet, le détruira.

Protocole

Le champ Protocole est codé sur 8 bits et représente le type de Data qui se trouve derrière l'entête IP.

- 01 – 00001 – ICMP
- 02 – 00010 – IGMP
- 06 – 00110 – TCP
- 17 – 10001 – UDP

Questions IP

Lancer la capture et faire une requête vers http://www.lequipe.fr/ avec le navigateur

Dans la capture prendre un message http continuation et développer IP

1. Quelle est la taille du message ?
2. Quelle la valeur de don't fragment ?
3. Quelle est la durée du TTL ?
4. Quel est le protocole de couche supérieur transporté dans IP ?

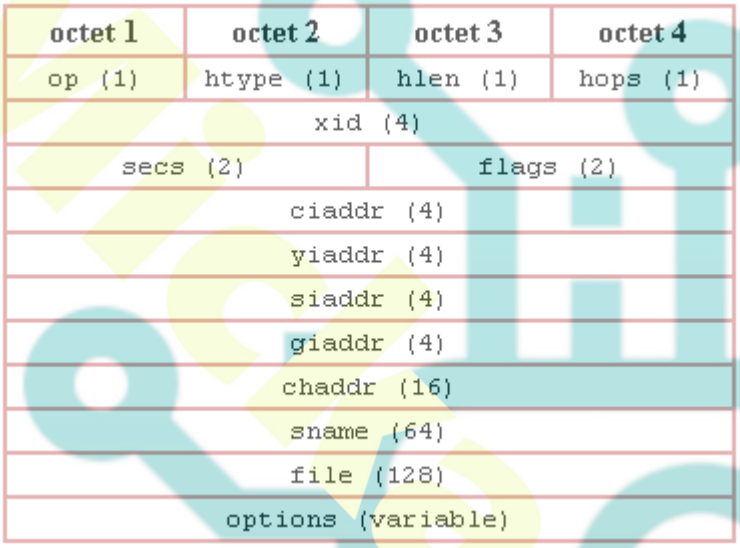
Lancer la capture et taper la commande suivante ping 8.8.8.8 -l 65000

1. Les paquets sont-ils fragmentés ?
2. Relancer la capture puis la commande suivante 8.8.8.8 -l 65000 -f
3. Que se passe-t-il ?
4. Relancer la capture puis la commande suivante ping 127.0.0.1
5. Qu'avez-vous capturé et pourquoi ?

Analyse DHCP

Format de la trame BOOTP/DHCP

La trame DHCP est en fait la même que BOOTP, et a le format suivant (les chiffres entre parenthèses indiquent la taille du champ en octets) :



octet 1	octet 2	octet 3	octet 4
op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (variable)			

- op : vaut 1 pour BOOTREQUEST (requête client), 2 pour BOOTREPLY (réponse serveur)
- htype : type de l'adresse hardware (adresse MAC)
- hlen : longueur de l'adresse hardware (en octet). C'est 6 pour une adresse MAC
- hops : peut être utilisé par des relais DHCP
- xid : nombre aléatoire choisi par le client et qui est utilisé pour reconnaître le client
- secs : le temps écoulé (en secondes) depuis que le client a commencé sa requête
- flags : flags divers
- ciaddr : adresse IP du client, lorsqu'il en a déjà une
- yiaddr : la (future ?) adresse IP du client
- siaddr : adresse IP du (prochain) serveur à utiliser
- giaddr : adresse IP du relai (passerelle par exemple) lorsque la connexion directe client/serveur n'est pas possible
- chaddr : adresse hardware du client
- sname : champ optionnel. Nom du serveur
- file : nom du fichier à utiliser pour le boot
- options : Champs réservé pour les options. Dans une précédente RFC, la taille de ce champ était limitée (limité à 64 octets par exemple pour la première version de Bootp) ; maintenant, il n'y a plus de limitation. Dans tous les cas, un client DHCP doit être prêt à recevoir au minimum 576 octets, mais la possibilité lui est offerte de demander au serveur de restreindre la taille de ses messages.

Questions DHCP

Démarrer l'analyse et lancer une machine de cours pour capturer des requêtes DHCP

Ouvrir une requête DHCP Discover

1. Quel est le type de message ?
2. Quel est le type de Hardware ?
3. Noter la valeur de la transaction
4. Le client utilise-t-il un agent relai ?
5. Connait-on l'adresse IP du serveur ?
6. Quelles sont les valeurs du champs client identifier ?
7. Quelles sont les valeurs du champs vendor identifier ?
8. Quels sont les paramètres demandés par le client ? (Parameter request list)

Rechercher l'offre du serveur (avec la même valeur de transaction) puis regarder les options

1. Quelle est l'adresse IP du serveur ?
2. Quelle est la durée du bail
3. Dans combien de temps de client va-t-il tenter de renouveler son bail ?
4. Quelle est l'adresse IP du routeur ?
5. Quelle est l'adresse IP du serveur DNS ?
6. Quelle est la valeur du masque de sous réseau ?

Quelle est l'adresse proposée par le serveur ?

Analyse DNS

Id

Codé sur 16 bits, doit être recopié lors de la réponse permettant à l'application de départ de pouvoir identifier le datagramme de retour.

FLAGS

- **Qr**
  Ce champ permet d'indiquer s'il s'agit d'une requête (0) ou d'une réponse (1).
- **Opcode**
  ce champ permet de spécifier le type de requête :
  - 0 – Requête standard (Query)
  - 1 – Requête inverse (Iquery)
  - 2 – Status d'une requête serveur (Status)
  - 3-15 – Réservé pour des utilisations futurs
- **Aa**
  Le flag Aa,signifie « Authoritative Answer ». Il indique une réponse d'une entité autoritaire.
- **Tc**
  Le champ Tc , indique que ce message a été tronqué.
- **Rd**
  Le flag Rd, permet de demander la récursivité en le mettant à 1.
- **Ra**
  Le flag Ra, indique que la récursivité est autorisée.
- **Z**
  Le flag Z, est réservé pour une utilisation future. Il doit être placé à 0 dans tous les cas. Désormais, cela est divisé en 3 bits : 1 bit pour Z, 1 bit pour AA (Authentificated Answer) qui indique si la réponse et authentifiée, et 1 bit NAD (Non-Authenticated Data) qui indique si les données sont non-authentifiées.
- **Rcode**
  Le champ Rcode, indique le type de réponse.
  - 0 – Pas d'erreur
  - 1 – Erreur de format dans la requête
  - 2 – Problème sur serveur
  - 3 – Le nom n'existe pas
  - 4 – Non implémenté
  - 5 – Refus
  - 6-15 – Réservés

Qdcount

Il spécifie le nombre d'entrée dans la section « Question ».

Ancount

Il spécifie le nombre d'entrée dans la section « Réponse ».

Nscount

Il spécifie le nombre d'entrée dans la section « Autorité ».

Arcount

Codé sur 16 bits, il spécifie le nombre d'entrée dans la section « Additionnel ».

Questions DNS

Lancer Wireshark et taper ping https://mickaelangel.com puis dans l'analyseur chercher le message DNS QUERY

1. Quelle est la valeur de la transaction ?
2. La récursivité est-elle demandée ?
3. Quel type de demande est effectuée (A, MX, CNAME, PTR ?)

Chercher le message DNS QUERY RESPONSE correspondant au DNS QUERY

1. La valeur de la transaction correspond-elle avec celle du query ?
2. Quelle est l'adresse IP v4 retournée ?
3. Y-a-t-il une réponse en ipv6 ?
4. Quelle est l'adresse IP v6 retournée ?

Analyse TCP

Port source TCP

Le champ Port source correspond au port relatif à l'application en cours sur la machine source.

Port destination TCP

Le champ Port destination correspond au port relatif à l'application en cours sur la machine de destination.

Numéro de séquence

Le champ Numéro de séquence correspond au numéro du paquet. Cette valeur permet de situer à quel endroit du flux de données le paquet, qui est arrivé, doit se situer par rapport aux autres paquets.

Numéro de l'accusé de réception

Le champ Numéro de séquence définit un acquittement pour les paquets reçus. Cette valeur signale le prochain numéro de paquet attendu. Par exemple, si'il vaut 1500, cela signifie que tous les Datagrammes <1500 ont été reçus

Offset

Ce champ indique donc où les données commencent.

Réservé

Le champ Réservé servira pour des besoins futurs. Ce champ doit être marqué à 0.

Flags

- Le champ URG indique que le champ Pointeur de donnée urgente est utilisé.
- Le champ ACK indique que le numéro de séquence pour les acquittements est valide.
- Le champ PSH indique au récepteur de délivrer les données à l'application et de ne pas attendre le remplissage des tampons.
- Le champ RST demande la réinitialisation de la connexion.
- Le champ SYN indique la synchronisation des numéros de séquence.
- Le champ FIN indique fin de transmission.

Voici certaines valeurs en hexa du champs Flags pour les combinaisons suivantes :

- 0x00 NULL, 0x01 FIN, 0x02 SYN,0x03 FIN-SYN,0x08 PSH, 0x10 ACK
- 0x12 SYN-ACK
- 0x18 PSH-ACK
- 0x19 FIN-PSH-ACK
- 0x1A SYN-PSH-ACK

Fenêtre

Le champ Fenêtre « Windows » correspond au nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir. Le destinataire ne doit donc pas envoyer les paquets après Numéro de séquence + Window.

Questions TCP

Lancer la capture et saisir la commande https://mickaelangel.com

1. Sélectionner le message http/get et développer TCP
2. Quel et le port source et quel est le port destination ?
3. A quoi correspondent-ils ?
4. Quelles est la valeur du flags ?
5. Quelle est la taille de la fenêtre ?
6. Dans la capture de trames, rechercher 3 messages TCP ayant la valeur syn, syn ack, ack
7. A quoi servent ces messages ?
8. Voyez-vous une logique dans les 3 messages avec les valeurs sequence number, Next séquence number et acknowledge number ?

Analyse UDP

Port source UDP

Le champ Port source est codé sur 16 bits et correspond au port relatif à l'application en cours sur la machine source.

Port destination UDP

Le champ Port destination correspond au port relatif à l'application en cours sur la machine de destination.

Longueur

Le champ Longueur représente la taille de l'entête et des données. Son unité est l'octet et sa valeur maximale est 64 Koctets (216).

Questions UDP

Lancer l'analyse et saisir la commande ping https://mickaelangel.com

1. Sélectionner le protocole DNS et développer UDP
2. Quel est le port source indiqué ?
3. Quel est le port destination indiqué ?

Analyse http

Allow

Le champ Allow liste l'ensemble des méthodes supportées par la ressource désignée par l'URI-visée. La fonction de ce champ est simplement d'informer le récepteur sur les méthodes qu'il peut utiliser sur la ressource.

1. Allow: GET, HEAD

Authorization

Un utilisateur désireux de s'identifier auprès d'un serveur-en général, mais pas nécessairement, après réception d'une réponse 401-peut le faire en incluant un champ d'en-tête Authorization dans sa nouvelle requête.

2. Authorization = "Authorization" ":" données_identification

Content-Encoding

Le champ Content-Encoding est utilisé pour compléter l'information de type de média. Il a été à l'origine instauré pour permettre la mise à disposition de ressource sous forme compressées, de sorte qu'il soit possible d'en connaître le type de média d'origine.

3. Content-Encoding: x-gzip

Content-Length

Le champ d'en-tête Content-Length indique la taille du corps sous la forme d'un nombre d'octets exprimé en décimal, envoyé au récepteur.

Content-Type

Le champ d'en-tête Content-Type indique le type de média envoyé au récepteur

4. Content-Type: text/html

Date

Le champ d'en-tête Date (général) donne la date et l'heure à laquelle le message a été "rédigé ».C'est un paramètre important pour tout ce qui touche à la gestion des caches.

Expires

Indique la date et l'heure à partir de laquelle le message doit être considéré comme obsolète. Ceci permet de suggérer la notion de "validité temporaire" de l'information. Les applications ne doivent pas enregistrer ces entités dans leur cache après la date spécifiée.

From

S'il est présent, il devra contenir l'adresse e-mail Internet de l'utilisateur "humain" contrôlant le client émetteur de la requête. Ce champ est exploité à des fins de statistiques, et pour identifier la source de requêtes non valides ou non autorisées.

If-Modified-Since

Est utilisé lors d'une requête de type GET pour en émettre une forme conditionnelle. Si la ressource visée n'a pas été modifiée depuis la date mentionnée dans ce champ, la copie de la ressource ne sera pas renvoyée par le serveur. Le but de cette implémentation est de permettre une remise à jour efficace des informations en cache, en réduisant au maximum les transactions réseau.

Last-Modified
Le champ d'en-tête Last-Modified (entité) indique la date et l'heure à laquelle le serveur pense que la ressource visée a été modifiée pour la dernière fois.

Location
Le champ d'en-tête Location (réponse) renvoie la localisation exacte de la ressource identifiée par l'URI-visée de la requête.

Pragma
Est utilisé pour transmettre des directives dépendantes de l'implémentation à tous les agents de la chaîne de requête/réponse. Lorsque la directive "no-cache" est présente dans un message de requête, les applications doivent répercuter la requête jusqu'au serveur origine, même si elles disposent d'une copie de la ressource en cache. Ceci permet au client de forcer la récupération d'une "première copie" d'une ressource. Ceci permet de plus de demander au client une remise à jour de copies cachées, dans le cas où ces copies se sont avérées défectueuses, ou obsolètes.

Referer
Permet au client d'indiquer, à l'usage du serveur, l'adresse (URI) de la ressource dans laquelle l'URI-visée a été trouvée. Ceci permet au serveur de générer et entretenir des listes de "rétro-liens" destinées à renseigner les clients futurs sur des "sites intéressants", ou à but d'archivage et d'analyse, optimisation de cache, etc.

Server
Le champ d'en-tête Server (réponse) contient des informations sur le logiciel utilisé par le serveur origine pour traiter la requête.

User-Agent
Contient des informations sur l'utilisateur émetteur de la requête.

WWW-Authenticate
Le champ d'en-tête WWW-Authenticate (réponse) doit être inclus dans des réponses de type 401 (non autorisé). La valeur du champ consiste en un ou plusieurs "modèles" d'identification pour l'URI-visée.

Questions HTTP

Lancer la capture et saisir la commande https://mickaelangel.com

1. Sélectionner le premier message http get correspondant à mickaelangel.com et securitycloud
2. Quel est le nom de l'host ?
3. Quelle est la valeur de user agent ?
4. Quel est le langage et le type de codage ?
5. Quelle est la valeur de cookie ?
6. Cliquer sur la réponse (reponse in frame xxx)
7. Quel est le type de sécurité demandé ?
8. Quel est le logiciel web utilisé par le serveur ?
9. Quelle est la version de PHP ?
10. Trouver la requête correspondant à securitycloud
11. Quel est le type de serveur web utilisé ?

Analyse SMTP

Delivered-to : Contient l'adresse e-mail du destinataire qui recevra le message.

Received, X-Received : Contient l'heure, la date d'envoi du message et le fuseau horaire utilisé.

Return-Path : Contient une adresse e-mail. Celle-ci recevra un message automatique si l'e-mail ne peut pas être délivré correctement (cf. adresse e-mail où sont envoyés les bounces)

Received : Contient les différentes informations techniques entre le serveur d'envoi du routeur et le serveur de messagerie du FAI/Webmail (IP utilisée pour l'envoi, nom du serveur de messagerie de Google, adresse e-mail du destinataire, heure & date d'envoi, etc.)

1. **Informations liées à l'authentification du message**

- **Received-SPF** : Contient le résultat de la signature SPF.
- **Authentication-Results** : Contient les résultats des signatures SPF/DKIM et de la norme DMARC.
- **DKIM-Signature** : Contient les données de la signature DKIM.

2. **Informations liées au routeur**

- **Date** : Contient la date, l'heure d'envoi du message ainsi que son fuseau horaire.
- **From** : Contient l'adresse expéditrice utilisée pour envoyer votre message.
- **Reply-to** : Contient l'adresse de réponse renseignée dans votre message.
- **To** : Contient l'adresse e-mail du destinataire qui recevra le message.
- **Message-ID** : Contient le numéro d'identification de l'e-mail.
- **Subject** : Contient l'objet de votre e-mail.
- **Mime-Version** : Contient la version du format de courrier utilisé (ici MIME, le format standard d'un courriel).
- **Content-Type** : Contient le type de message envoyé (ici format multipart : html/txt).
- **X-EMV…** : Contient différentes informations du routeur (par exemple : son nom, la plateforme ou serveur utilisé, l'id de la campagne ou encore l'id de l'utilisateur ciblé).
- **List-Unsubscribe** : Contient les informations (généralement une adresse e-mail et un lien de désabonnement) pour se désabonner du mailing (ces informations peuvent être utilisées par un utilisateur ou par un système de désabonnement automatique d'un FAI – par exemple SFR avec Vade Retro Unsubscribe).
- **List-Id** : Contient le numéro d'identification de votre mailing list.

Questions SMTP

1. Ouvrir le message envoyé par pierre hier
2. Afficher les en têtes
3. Copier l'en-tête dans le lien suivant https://mxtoolbox.com/EmailHeaders.aspx
4. Quel serveur qui a envoyé le message ?
5. Quel serveur a réceptionné le message ?
6. Quelle est l'adresse IP du serveur ?
7. Quelle est l'adresse IP du client ?
8. Le message est-il protégé contre les virus

Analyse FTP

Questions FTP

1. Lancer l'analyse
2. Dans l'invite de commandes taper **ftp ftp.dlptest.com**
3. Indiquer l'utilisateur suivant **dlpuser@dlptest.com**
   et mot de passe suivant **puTeT3Yei1IJ4UYT7q0r**
4. Chercher le ligne FTP REQUEST USER
5. Quel protocole est utilisé pour transporter le protocole FTP ?
6. Quel est le port client et serveur ?
7. Dans la capture trouver le mot de passe saisie
8.

Analyse SSL/TLS

1. Lancer l'analyse
2. Accéder au site https//mickaelangel.com
3. Dans la capture repérer TLS v1.3 et php du serveur
4. Quel type de chiffrement est proposé par le server (cipher suite)
5. Quelle est la clé publique (Diffie Hellman param)
6. Trouver une ligne avec information php
7. Quels types d'algo de hachage supporte le client ? (extension signature algo)

Analyse SMB

Se connecter à un serveur Windows et rechercher TREE CONNECT